Revista de investigación de sistemas e informática
17(2): 185-193 (2024)
DOI: https://doi.org/10.15381/risi.v17i2.29659

ISSN: 1815-0268 (Impreso) / ISSN: 1816-3823 (Electrónico)
Facultad de Ingeniería de Sistemas e Informática - UNMSM

Impacto de tecnologías emergentes de ciberseguridad en la gestión de incidentes: un análisis sistemático

Impact of cybersecurity emerging technologies on incident management: a systematic analysis

Alejandro Felipe Hernández Legua
https://orcid.org/0009-0007-8871-9720
alejandro.hernandez1@unmsm.edu.pe
Universidad Nacional Mayor de San Marcos, Lima, Perú

Recibido: 06/12/2024 - Aceptado: 15/12/2024 - Publicado: 31/12/2024

RESUMEN

En este estudio de revisión sistemática, se aborda la evaluación de la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad. Se llega a destacar la diversidad de enfoques y prácticas utilizadas, incluyendo como es posible llegar a la colaboración entre entidades públicas y privadas, así como hasta el uso de tecnologías emergentes en el sector educativo. Para conseguirlo, la metodología empleada en esta revisión se basó en el método PRISMA para garantizar la transparencia y calidad en la revisión de la literatura científica. Posteriormente en el desarrollo del documento, los resultados revelan la importancia de seguir investigando y mejorando las estrategias de respuesta a incidentes en entornos empresariales digitalizados, así como estar a la vanguardia en la búsqueda de nuevas tecnologías constantemente debido a la evolución de las amenazas digitales. La conclusión más relevante del estudio destaca la necesidad de explorar en futuras investigaciones el impacto de la colaboración público-privada y las tecnologías emergentes en la ciberseguridad empresarial, las cuales nos ofrecen nuevas perspectivas para fortalecer la seguridad cibernética en un entorno en constante evolución. Este estudio aporta una visión actualizada y crítica sobre la gestión de incidentes cibernéticos en organizaciones tecnológicamente avanzadas.

Palabras claves: Estrategias de respuesta, Tecnologías emergentes, Ciberseguridad, Organizaciones, Efectividad.

ABSTRACT

This systematic review study addresses the evaluation of the effectiveness of incident response strategies in organizations with emerging cybersecurity technologies. It highlights the diversity of approaches and practices used, including how it is possible to achieve collaboration between public and private entities, as well as the use of emerging technologies in the educational sector. To achieve this, the methodology used in this review was based on the PRISMA method to ensure transparency and quality in the review of scientific literature. Later in the development of the document, the results reveal the importance of continuing to research and improve incident response strategies in digitalized business environments, as well as being at the forefront in the constant search for new technologies due to the evolution of digital threats. The most relevant conclusion of the study highlights the need to

explore in future research the impact of public-private collaboration and emerging technologies on business cybersecurity, which offer us new perspectives to strengthen cybersecurity in a constantly evolving environment. This study provides an updated and critical view on cyber incident management in technologically advanced organizations.

Keywords: Response strategies, Emerging technologies, Cybersecurity, Organizations, Effectiveness.

1. INTRODUCCIÓN

La ciberseguridad en las organizaciones ha adquirido una relevancia crítica en un entorno digital cada vez más complejo y expuesto a amenazas cibernéticas. En este contexto, la efectividad de las estrategias de respuesta a incidentes se convierte en un factor determinante para garantizar la protección de la información y la continuidad de las operaciones. Según (Quintero et al., 2018), la competencia docente en el mundo digital requiere un replanteamiento constante para adaptarse a las demandas cambiantes de la era digital. En este sentido, la gestión estratégica, como señalan González et al. (2019), se convierte en una herramienta fundamental para la toma de decisiones en las organizaciones, incluyendo aquellas relacionadas con la ciberseguridad.

En investigaciones recientes, se ha abordado la importancia de la ciberseguridad en diversos contextos. Por ejemplo, Font (2010) propone una pauta para el análisis e intervención a través de incidentes críticos en la formación del profesorado, destacando la relevancia de abordar situaciones inesperadas para fortalecer la identidad profesional. Sin embargo, a pesar de estos avances, existen vacíos en la literatura actual que justifican la necesidad de evaluar la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad. En este sentido, estudios como el de Romero & Mercado (2018) sobre las estrategias de ciberseguridad en países latinoamericanos resaltan la importancia de abordar de manera efectiva los desafíos en la gestión de incidentes en entornos tecnológicamente avanzados.

Por otra parte, la creciente dependencia de las pequeñas y medianas empresas (PYMES) en la tecnología y el uso intensivo de internet han generado nuevas oportunidades para optimizar sus operaciones, consiguiendo una mejora en la interacción con los clientes y poder expandir sus mercados. Sin embargo, este mismo avance tecnológico las expone a una serie de vulnerabilidades cada vez más sofisticadas frente al cibercrimen. Estas amenazas ponen en riesgo la seguridad de sus datos sensibles, lo que puede derivar en pérdidas económicas, daños reputacionales y sanciones regulatorias severas (Bustillos et al, 2022).

Diversos estudios obtenidos por los autores mencionados (2022) han señalado que, aunque muchas PYMES son conscientes de los riesgos cibernéticos, pocas cuentan con protocolos efectivos para mitigar estos desafíos. Esto subraya la necesidad urgente de desarrollar soluciones accesibles y escalables que permitan a estas organizaciones proteger sus activos digitales y garantizar la continuidad de sus operaciones en un entorno cada vez más interconectado y digitalizado.

Al poder abordar este problema, no solo se contribuiría a la sostenibilidad y resiliencia de las PYMES, sino también al fortalecimiento de los ecosistemas económicos locales y globales. También, (Rodriguez, 2023) explica que a medida que las transacciones financieras evolucionan hacia modelos más complejos y las organizaciones adoptan sistemas tecnológicos avanzados, los perpetradores del fraude también han desarrollado técnicas cada vez más sofisticadas para eludir los controles establecidos. Así, la necesidad de implementar defensas robustas contra el fraude financiero se vuelve apremiante. Este desafío no se limita únicamente a fortalecer los controles tradicionales, sino que también exige una modernización integral de las capacidades organizativas de detección y prevención. El autor destaca el uso de auditoría forense en conjunto con la inteligencia artificial para conseguir ese objetivo.

Tampoco se debe descartar el desarrollo propio de tecnologías alternativas con objetivos académicos pero que aportan igualmente a la causa, tal como el caso de (Almeida et al, 2023) el cual desarrolló un estudio fundamentado en el análisis de una base de datos proporcionada por la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de los Estados Unidos, una fuente clave que documenta incidentes de ciberseguridad dentro del sector de la salud. Para llevar a cabo su análisis, se optó por emplear la metodología KDD (Knowledge Discovery in Databases), el cual le permitió extraer conocimiento útil y comprensible a partir de grandes volúmenes de datos. Este proceso, se considera especialmente valioso en el campo de la minería

de datos, ya que permite descubrir patrones válidos y novedosos que pueden ser aplicados para mejorar las estrategias de ciberseguridad.

Por consiguiente y con algunas de las introducciones mencionadas anteriormente, el objetivo de este artículo de revisión sistemática es evaluar la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad. Este objetivo se fundamenta en la necesidad de abordar los vacíos identificados en la literatura actual y contribuir al avance del conocimiento en el campo de la ciberseguridad, ofreciendo una visión crítica y actualizada sobre la gestión de incidentes en entornos tecnológicamente avanzados.

2. MÉTODOS

Para llevar a cabo esta revisión sistemática, se siguió el método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Se establecieron las etapas clave del proceso, que incluyen la identificación, selección, evaluación y síntesis de los estudios relevantes. Siguiendo las directrices de PRISMA, se realizó una búsqueda exhaustiva de la literatura científica para identificar estudios pertinentes que aborden la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad.

Para guiar la revisión sistemática, se formularon las siguientes preguntas de investigación:

a. ¿Cuáles son las estrategias de respuesta a incidentes más comúnmente utilizadas en organizaciones con tecnologías emergentes en ciberseguridad?

b. ¿Qué evidencia existe sobre la efectividad de estas estrategias en la gestión de incidentes cibernéticos?

c. ¿Cómo se comparan las diferentes estrategias en términos de su impacto en la resolución de incidentes?

d. ¿Qué factores influyen en la efectividad de las estrategias de respuesta a incidentes en entornos tecnológicamente avanzados?

e. ¿Existen brechas o áreas de mejora identificadas en la literatura en relación con la gestión de incidentes en organizaciones con tecnologías emergentes?

Se realizaron búsquedas en bases de datos académicas como PubMed, Scopus y Web of Science utilizando términos clave como "ciberseguridad", "tecnologías emergentes", "estrategias de respuesta a incidentes", entre otros. Se incluyeron estudios publicados en los últimos cinco años en revistas científicas indexadas y revisadas por pares. Se consideraron artículos en español e inglés para abarcar un espectro amplio de investigaciones relevantes.

Ahora, la generación de la cadena de búsqueda fue clave en la revisión sistemática, siguiendo las directrices del método PRISMA, se identificaron los términos clave para esta investigación y sus combinaciones para abarcar un espectro amplio de investigaciones pertinentes. Inicialmente, se definieron conceptos centrales basados en las preguntas de investigación, tales como ciberseguridad, tecnologías emergentes, gestión de incidentes, y estrategias de respuesta. Estos términos se ampliaron utilizando sinónimos y variaciones contextuales. Por ejemplo: Se incluyeron expresiones como "incident management", "emerging technologies", y "incident response frameworks" para abarcar diferentes enfoques lingüísticos y técnicos. También, se incorporaron operadores booleanos (AND, OR, NOT) para construir cadenas complejas que combinaran conceptos relacionados.

La cadena de búsqueda final, adaptada a las especificaciones de cada base de datos académica, incluyó variaciones como:

- "cybersecurity" AND "emerging technologies" AND "incident response"
- "blockchain" OR "artificial intelligence" AND "incident management"
- "data mining" AND "incident detection"

Los criterios de exclusión se aplicaron para descartar estudios que no estuvieran relacionados directamente con la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad. Se excluyeron estudios que no abordaban específicamente la gestión de incidentes cibernéticos o que no proporcionaban información relevante para la evaluación de estrategias en entornos tecnológicamente avanzados.

Igualmente, los criterios de inclusión se definieron siguiendo las buenas prácticas especificadas por PRISMA y fueron plasmadas en la siguiente tabla:

Tabla 1

Criterios de Inclusión y Exclusión para el Artículo Científico

Criterios de Inclusión	Criterios de Exclusión
Enfoque temático: Se seleccionaron estudios que aborden estrategias de respuesta a incidentes de ciberseguridad en empresas y su efectividad en el contexto de tecnologías emergentes, como blockchain, inteligencia artificial y Big Data.	Irrelevancia temática: Se descartaron estudios que no estuvieran directamente relacionados con la gestión de incidentes o que solo abordaran aspectos tangenciales, como políticas organizativas generales o marcos de trabajo sin énfasis en incidentes.
Relevancia temporal: Solo se incluyeron investigaciones publicadas en los últimos cinco años (2019-2024), asegurando que los hallazgos sean actuales y relevantes para el entorno tecnológico dinámico.	Contexto no alineado: Investigaciones centradas exclusivamente en sectores no tecnológicos o en contextos no aplicables a organizaciones modernas fueron excluidas.
Calidad académica: Se consideraron artículos publicados en revistas científicas indexadas y revisadas por pares, garantizando la rigurosidad metodológica de las fuentes.	Limitaciones metodológicas: Artículos con descripciones inconclusas de los métodos utilizados o sin evaluación cuantitativa o cualitativa de las estrategias presentadas fueron eliminados del análisis.
Idiomas: Se incluyeron estudios en inglés y español para ampliar la diversidad de las fuentes y abarcar investigaciones regionales y globales.	Documentos duplicados: Se excluyeron duplicados identificados en múltiples bases de datos, manteniendo solo las versiones completas y originales.

Fuente: Elaboración propia.

Después de haber aplicado los criterios de inclusión y exclusión a la revisión de la literatura obtenida, un total de 53 artículos se fue optimizando hasta obtener actualmente un total de 20 artículos para su estudio.

Este enfoque metodológico riguroso permitirá realizar una revisión sistemática exhaustiva y objetiva de la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad, contribuyendo así al avance del conocimiento en este campo crucial de la ciberseguridad empresarial.

La revisión de literatura, la cual es una herramienta esencial en la investigación científica, permitió identificar las tecnologías emergentes más relevantes y sus aplicaciones en la ciberseguridad actual. También se consultaron las bases de datos académicas de alta relevancia citadas por los autores, como IEEE, ScienceDirect y Google Scholar, y se revisó que seleccionaron artículos entre 2019 y 2023. Aparte de la metodología ya utilizada, se encontraron documentos que abordan temas importantes sobre blockchain, inteligencia artificial (IA), Big Data, y ciberseguridad aplicada a incidentes críticos.

Gracias a esta fase, se me permitió mapear las tecnologías clave, así como también identificar tendencias emergentes en el campo de la ciberseguridad que han de funcionar para la posteridad, como el uso de aprendizaje profundo y la transferencia de aprendizaje (Yagual et al., 2022). Para dar un ejemplo, la combinación de blockchain con contratos inteligentes destacó como un área prometedora para la auditoría continua y la automatización en sectores como la salud y la industria financiera (Macías et al., 2020).

Así como se puede rescatar el diseño de una arquitectura de tres capas el cual se basó en la integración de tecnologías como Big Data, plataformas de inteligencia de amenazas y algoritmos de inteligencia artificial (Narváez et al., 2021). La primera capa, de detección, emplea herramientas como Suricata y Snort para el monitoreo en tiempo real del tráfico de red, mientras que la capa de nube almacena y analiza datos mediante algoritmos como RANDOM FOREX, seleccionados por su alta precisión. Finalmente, la capa de aplicación gestiona la visualización y respuesta a los incidentes. Esta metodología, inspirada en el trabajo con dispositivos IoT, utiliza hardware económico, como el Raspberry Pi 3, para garantizar la viabilidad económica de la solución (Narváez et al, 2021).

También se rescatan las aplicaciones en técnicas de minería de datos, como la metodología KDD (Knowledge Discovery in Databases), para identificar patrones en datos históricos de infracciones cibernéticas (Yagual et al, 2022). El uso de algoritmos avanzados, como las redes neuronales recurrentes (RNN) y las redes de memoria a corto plazo (LSTM), permitió abordar problemas complejos como la detección de intrusos y la predicción de ciberataques (Yagual et al., 2022). Además, el aprendizaje profundo por transferencia (DTL) facilitó el entrenamiento de modelos en escenarios con datos limitados, demostrando ser una herramienta poderosa para mejorar la precisión en tareas como la detección de malware y phishing (Yagual et al., 2022).

Finalmente, para adaptarse a las necesidades específicas de pequeñas y medianas empresas, se encontró que se desarrolló un protocolo básico de ciberseguridad que incluye la definición de perfiles de usuario, políticas de privacidad, y el uso de firewalls y antivirus (Ortega et al., 2022). Este enfoque busca fomentar una cultura de seguridad accesible y efectiva, alineada con normas internacionales como ISO/IEC 27001.

3. RESULTADOS

La cuantificación y obtención de los resultados de la investigación se presentará en tablas donde cada una nos brinda la respuesta más cercana a cada pregunta planteada en el capítulo de métodos, resaltando lo esencial de sus investigaciones y las oportunidades de mejoras por cada sección.

Tabla 2

Resultados de la Primera Pregunta de Investigación

1. ¿Cuáles son las estrategias de respuesta a incidentes más comúnmente utilizadas en organizaciones con tecnologías emergentes en ciberseguridad?	
Fuente:	Hueso & Acevedo (2021)
Metodología:	Análisis de datos secundarios
Conclusión Principal:	La guía de ciberseguridad para ciudades inteligentes destaca la importancia de la colaboración público-privada en la implementación de estrategias efectivas.

Fuente: Elaboración propia

Gracias al artículo sabemos que las organizaciones que operan en entornos urbanos con tecnologías emergentes están adoptando enfoques integrales para garantizar la ciberseguridad de sus infraestructuras físicas y digitales. Un ejemplo destacado es el trabajo del grupo temático de Ciudades Inteligentes y Datos Cívicos de la División de Vivienda y Desarrollo Urbano del Banco Interamericano de Desarrollo (BID). Entre las iniciativas clave implementadas se encuentran estudios, proyectos piloto y herramientas de autoevaluación en sectores estratégicos como la energía, la salud y las ciudades. Estas herramientas no solo permiten evaluar los niveles actuales de preparación y prevención ante ciberataques, sino también identificar áreas de mejora que pueden guiar futuras estrategias de fortalecimiento de capacidades. Este tipo de estrategias refleja una visión proactiva que no solo busca mitigar los riesgos inmediatos, sino también establecer bases sólidas para un crecimiento urbano sostenible.

Tabla 3

Resultados de la Segunda Pregunta de Investigación

2. ¿Qué evidencia existe sobre la efectividad de estas estrategias en la gestión de incidentes cibernéticos?	
Fuente:	Salinas (2023)
Metodología:	Estudio de caso
Conclusión Principal:	La auditoría forense en la era de la inteligencia artificial es un enfoque vanguardista para combatir el fraude financiero.

Fuente: Elaboración propia

Se sabe que la evidencia sobre la efectividad de las estrategias en la gestión de incidentes cibernéticos señala que la auditoría forense ha emergido como una herramienta fundamental no solo para identificar fraudes pasados, sino también para prevenir y disuadir futuras actividades ilícitas. Su evolución hacia el uso de técnicas de análisis de datos avanzadas y la incorporación de tecnologías innovadoras, como la inteligencia artificial (IA) y el aprendizaje automático, ha demostrado ser una defensa eficaz en un entorno empresarial donde las amenazas cibernéticas y los métodos de fraude financiero son cada vez más sofisticados.

Otro factor clave para la efectividad de estas estrategias es la educación continua y la colaboración interdisciplinaria. La interacción entre analistas de datos, expertos en ciberseguridad y auditores forenses resulta esencial para abordar la complejidad de los incidentes cibernéticos. Mantenerse actualizado sobre las últimas tendencias y tecnologías mediante programas de formación especializada asegura que los profesionales estén equipados para enfrentar desafíos emergentes.

Tabla 4

Resultados de la Tercera Pregunta de Investigación

3. ¿Cómo se comparan las diferentes estrategias en términos de su impacto en la resolución de incidentes?	
Fuente:	Almeida (2023)
Metodología:	Análisis de datos secundarios
Conclusión Principal:	Mejorar la seguridad cibernética en el sector de la salud es crítico para mitigar futuros riesgos.

Fuente: Elaboración propia

Se conoce que las diferentes estrategias de respuesta a incidentes pueden compararse en términos de su impacto en la resolución de incidentes considerando aspectos como la efectividad frente a vectores de ataque específicos, la capacidad de mitigación de riesgos y la adaptabilidad a tendencias

emergentes. En el caso de HCA Healthcare, con 11,270,000 individuos afectados, y los 562 incidentes registrados entre proveedores de atención médica, subraya la importancia de adoptar medidas específicas para cada tipo de amenaza.

Las estrategias que integran tecnologías emergentes como inteligencia artificial, análisis de Big Data y sistemas avanzados de monitoreo destacan por su impacto superior en la detección temprana de amenazas y la reducción de su alcance.

Tabla 5

Resultados de la Cuarta Pregunta de Investigación

4. ¿Qué factores influyen en la efectividad de las estrategias de respuesta a incidentes en entornos tecnológicamente avanzados?	
Fuente:	Macías et al (2020)
Metodología:	Estudio de caso
Conclusión Principal:	Destacar el uso de blockchain y contratos inteligentes ha demostrado su capacidad para automatizar auditorías y optimizar procesos críticos.

Fuente: Elaboración propia

La efectividad de las estrategias de respuesta a incidentes en entornos tecnológicamente avanzados está influenciada por una serie de factores interrelacionados que van desde la adopción de tecnologías innovadoras hasta la integración en discusiones y colaboraciones internacionales. En este contexto, la tecnología Blockchain emerge como un componente clave que no solo ofrece soluciones técnicas para la trazabilidad y la seguridad, sino que también abre nuevas oportunidades para el avance del conocimiento y la colaboración global en ciberseguridad. Uno de los principales factores identificados es la capacidad de las organizaciones y académicos para integrarse tempranamente en discusiones internacionales sobre las aplicaciones de tecnologías emergentes. Este enfoque colaborativo no solo fomenta el intercambio de mejores prácticas, sino que también amplía las perspectivas al incluir contextos locales y regionales dentro de un marco global.

Otro aspecto relevante es la necesidad de superar el conservadurismo exhibido por algunas organizaciones, adoptando enfoques más innovadores y alineados con las tendencias tecnológicas actuales. La formación continua y el acceso a conocimientos especializados son fundamentales para garantizar que tanto los profesionales como los estudiantes estén preparados para abordar los desafíos que presentan los entornos tecnológicos avanzados. En conjunto, estos factores destacan la importancia de combinar innovación tecnológica, colaboración interdisciplinaria y un compromiso con la formación continua para maximizar la efectividad de las estrategias de respuesta a incidentes.

Tabla 6

Resultados de la Quinta Pregunta de Investigación

5. ¿Existen brechas o áreas de mejora identificadas en la literatura en relación con la gestión de incidentes en organizaciones con tecnologías emergentes?	
Fuente:	Bustillos et al. (2022)
Metodología:	Estudio de caso
Conclusión Principal:	Proponer un protocolo básico de ciberseguridad que permita la continuidad del negocio en caso de un ataque cibernético

Fuente: Elaboración propia

Aunque muchas PYMES son conscientes de la importancia de la ciberseguridad, esta no ha sido una prioridad significativa en sus agendas estratégicas (Benz & Chatterjee, 2020). Esto se refleja en la persistencia de fallas y vulnerabilidades, a pesar de los crecientes ataques cibernéticos. Una de las razones principales es la percepción de que las medidas de ciberseguridad son complejas, costosas y requieren un nivel técnico avanzado, lo que desincentiva su adopción.

Las brechas también incluyen la insuficiencia de medidas de seguridad informática, la falta de capacitación del personal y la ausencia de políticas robustas de gestión de riesgos. Estas deficiencias tienen un impacto directo en la continuidad del negocio y la capacidad de las empresas para cumplir con sus objetivos organizacionales. Para abordar estas áreas de mejora, se destaca la importancia de una adecuada gestión de recursos, incluso en contextos de limitaciones. Las PYMES deben priorizar la protección de su activo más valioso, la información. La implementación de protocolos básicos de ciberseguridad puede servir como un paso inicial sólido hacia la construcción de una cultura organizacional que valore y priorice la seguridad cibernética.

Estos resultados proporcionan una visión amplia y detallada sobre las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad, destacando la diversidad de enfoques y la importancia de la efectividad en la gestión de incidentes cibernéticos.

4. DISCUSIÓN

Al comparar los resultados obtenidos en este estudio con la literatura existente, se observa que las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad han sido abordadas de manera diversa en investigaciones previas. Por ejemplo, el estudio de Zambrano et al. (2023) destaca la importancia de las tecnologías educativas emergentes para fortalecer el proceso de enseñanza-aprendizaje, lo cual podría tener implicaciones en la adopción de estrategias innovadoras en el ámbito de la ciberseguridad. En contraste, la guía de ciberseguridad para ciudades inteligentes de Hueso & Acevedo (2021) resalta la colaboración público-privada como un factor clave en la implementación efectiva de estrategias de ciberseguridad.

Una limitación importante de este estudio radica en la disponibilidad limitada de investigaciones específicas que aborden directamente la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad. Esto podría afectar la generalización de los hallazgos y la profundidad del análisis comparativo. Además, la heterogeneidad en los enfoques metodológicos de los estudios revisados podría haber introducido sesgos en la síntesis de los resultados.

Considerando las limitaciones identificadas, se sugiere que futuras investigaciones en este campo se enfoquen en la realización de estudios empíricos que evalúen de manera más directa la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad. Además, se recomienda explorar en mayor profundidad el impacto de la colaboración público-privada en la implementación de estas estrategias, así como investigar el papel de las tecnologías educativas emergentes en la formación de profesionales de ciberseguridad. Estas áreas podrían ofrecer nuevas perspectivas y enfoques para fortalecer la seguridad cibernética en entornos empresariales en constante evolución.

A pesar de las limitaciones identificadas, este estudio proporciona una base sólida para futuras investigaciones en el campo de la ciberseguridad, destacando la importancia de evaluar y mejorar continuamente las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes.

Para añadir a la discusión de estos hallazgos, en este apartado nos centramos en las implicaciones, desafíos y oportunidades que presentan las tecnologías emergentes: Para poder adaptar tecnologías como IA y blockchain se requiere considerar aspectos éticos, como la privacidad de datos y la transparencia en la toma de decisiones automatizadas. En particular, en sectores sensibles como la salud, la implementación de estas tecnologías debe alinearse con regulaciones estrictas para evitar vulnerabilidades legales y de seguridad (Almeida et al, 2023).

La arquitectura de tres capas diseñada para dispositivos IoT integró eficientemente tecnologías avanzadas, logrando una mejora notable en la detección de amenazas y la reducción de latencia. La elección del hardware Raspberry Pi 3 permitió balancear el rendimiento y el costo, haciéndolo accesible incluso para empresas pequeñas (Narváez et al, 2021).

El aprendizaje profundo alcanzó una precisión del 99.5% en la detección de ciberataques, superando los métodos tradicionales. La transferencia de aprendizaje permitió que los modelos aprendieran de conjuntos de datos reducidos, acelerando los tiempos de implementación sin sacrificar precisión (Yagual et al, 2022).

Si bien las PYMES tienen acceso a soluciones prácticas, su capacidad para implementar estas tecnologías se ve limitada por restricciones de presupuesto y conocimientos técnicos. Además, el cambio cultural necesario para adoptar una visión proactiva en ciberseguridad representa un reto significativo (Ortega et al., 2022).

Las arquitecturas propuestas superan en eficiencia y precisión a los modelos tradicionales, aunque enfrentan desafíos relacionados con la escalabilidad y la personalización para contextos locales (Narváez et al, 2021).

5. CONCLUSIONES

En este artículo de revisión sistemática, se han identificado y analizado los principales hallazgos relacionados con la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad. Se ha observado una diversidad de enfoques y prácticas utilizadas en la gestión de incidentes cibernéticos, destacando la importancia de la colaboración público-privada y el uso de tecnologías educativas emergentes. Estos resultados contribuyen significativamente al campo de estudio de la ciberseguridad empresarial al proporcionar una visión amplia y actualizada sobre las estrategias efectivas en entornos tecnológicamente avanzados.

El objetivo planteado en este artículo de revisión sistemática, que consistía en evaluar la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad, ha sido abordado de manera exhaustiva y crítica. A través del análisis de la literatura científica actual, se ha logrado identificar las tendencias, desafíos y oportunidades en la gestión de incidentes cibernéticos en entornos empresariales modernos y tecnológicamente avanzados.

Este artículo se enmarca dentro del tipo de estudio de revisión sistemática, que ha permitido sintetizar y analizar de manera rigurosa la evidencia disponible sobre la efectividad de las estrategias de respuesta a incidentes en organizaciones con tecnologías emergentes en ciberseguridad. La metodología utilizada ha seguido las directrices del método PRISMA, garantizando la transparencia y la calidad en la revisión de la literatura científica.

Así, este estudio destaca la importancia de seguir investigando y mejorando las estrategias de respuesta a incidentes en un contexto empresarial cada vez más digitalizado y expuesto a amenazas cibernéticas. Se sugiere que futuras investigaciones se enfoquen en la realización de estudios empíricos que evalúen la efectividad de estas estrategias en la práctica, así como en explorar el impacto de la colaboración público-privada y el uso de tecnologías emergentes en la ciberseguridad empresarial. Estas áreas podrían ofrecer nuevas perspectivas y enfoques para fortalecer la seguridad cibernética y proteger la información en entornos empresariales en constante evolución.

Para concluir, y con base en la metodología aplicada y los resultados obtenidos, las tecnologías emergentes, como blockchain e IA, no solo transforman los métodos actuales, sino que también abren nuevas posibilidades para prevenir y responder a incidentes de manera más efectiva. No olvidar que es crucial desarrollar soluciones adaptadas a las necesidades específicas de diferentes sectores y tamaños de organizaciones, desde grandes hospitales hasta PYMES. Noción especial a que se debe profundizar en la investigación de tecnologías como la auditoría continua y el aprendizaje profundo, así como en la creación de marcos regulatorios que equilibren innovación y seguridad. Y que es necesario la combinación de expertos en tecnología, ética y gestión empresarial es esencial para maximizar el impacto positivo de estas tecnologías.

REFERENCIAS

[1] Almeida, J. C., Loor, J. V., Pisco, X. M., & Guaña-Moya, J. (2023a). Análisis de patrones y tendencias de las infracciones en ciberseguridad en un departamento de salud y servicios humanos. Revista Tecnopedagogía e Innovación, 2(2), 27–46. https://doi.org/10.62465/RTI.V2N2.2023.55

[2] Almeida, J. C., Loor, J. V., Pisco, X. M., & Guaña-Moya, J. (2023b). Análisis de patrones y tendencias de las infracciones en ciberseguridad en un departamento de salud y servicios humanos. Revista Tecnopedagogía e Innovación, 2(2), 27–46. https://doi.org/10.62465/RTI.V2N2.2023.55

[3] Antonio, J. M. A. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales, 53(198), 169–197. https://doi.org/10.5354/0719-3769.2021.57067

[4] Ciapponi, A. (2021). La declaración PRISMA 2020: una guía actualizada para reportar revisiones sistemáticas. Evidencia - Actualización En La Práctica Ambulatoria, 24(3), e002139–e002139. https://doi.org/10.51987/EVIDENCIA.V24I4.6960

[5] Hueso, L. C., & Acevedo, M. S. (2021). Guía de ciberseguridad para ciudades inteligentes. Guía de Ciberseguridad Para Ciudades Inteligentes. https://doi.org/10.18235/0003876

[6] M., J. J. C. (2020). Seguridad y ciberseguridad 2009-2019. Revista Sistemas, 155, 81–94. https://doi.org/10.29236/SISTEMAS.N155A6

[7] Macias, H. A., Farfán, M. A., & Rodríguez, B. A. (2020). Contabilidad digital: los retos del blockchain para académicos y profesionales. Revista Activos, 18(1). https://doi.org/10.15332/25005278/6152

[8] Mendoza-Zambrano, M. G., De-la-Peña-Consuegra, G., & Linzán-Saltos, M. F. (2023). Tecnologías educativas emergentes para fortalecer el proceso de enseñanza-aprendizaje en los estudiantes de tercero Bachillerato en tiempos de pandemia. MQRInvestigar, 7(1), 54–73. https://doi.org/10.56048/MQR20225.7.1.2023.54-73

[9] Narváez, J. J. C., Villalba, K. M., & Donado, S. A. (2021). Arquitectura basada en tecnologías emergentes y monitoreo de tráfico de red. Investigación e Innovación En Ingenierías,

9(3), 18–31. https://doi.org/10.17081/INVINNO.9.3.5340

[10] Ortega, O. B., & Segura, J. R. (2022). Protocolo básico de ciberseguridad para pymes. Interfases, 016, 168–186. https://doi.org/10.26439/INTERFASES2022.N016.6021

[11] Pinargote, O. S. B., Chóez, J. A. A., Manrique, C. D. C., & Plúa, C. R. C. (2024a). Políticas de seguridad en la infraestructura tecnológica de instituciones de salud mediante un appliance fortinet 80e: Estudio de caso Hospital Básico Jipijapa. Revista Científica de Salud BIOSANA, 4(1), 115–138. https://doi.org/10.62305/BIOSANA.V4I1.102

[12] Pinargote, O. S. B., Chóez, J. A. A., Manrique, C. D. C., & Plúa, C. R. C. (2024b). Políticas de seguridad en la infraestructura tecnológica de instituciones de salud mediante un appliance fortinet 80e: Estudio de caso Hospital Básico Jipijapa. Revista Científica de Salud BIOSANA, 4(1), 115–138. https://doi.org/10.62305/BIOSANA.V4I1.102

[13] Romero, R. J. G., & Mercado, A. G. V. (2018). Las mipymes tecnológicas peruanas al 2030. Estrategias para su inserción a la industria 4.0. Nova Scientia, 10(20), 754–778. https://doi.org/10.21640/NS.V10I20.1329

[14] Salinas, J. R. (2023a). Auditoría forense en la era de la inteligencia artificial, un enfoque vanguardista para combatir el fraude financiero. Punto de Vista, 14(21). https://doi.org/10.15765/PDV.V14I21.4051

[15] Salinas, J. R. (2023b). Auditoría forense en la era de la inteligencia artificial, un enfoque vanguardista para combatir el fraude financiero. Punto de Vista, 14(21). https://doi.org/10.15765/PDV.V14I21.4051

[16] Salinas, J. R. (2023c). Auditoría forense en la era de la inteligencia artificial, un enfoque vanguardista para combatir el fraude financiero. Punto de Vista, 14(21). https://doi.org/10.15765/PDV.V14I21.4051

[17] Tasa-Catanzaro, M. E., Maquera-Quispe, H. G., Rojas-Bujaico, J. F., & Delgado-Rospigliosi, M. G. del C. (2022a). Análisis de información de la gestión de incidentes de seguridad en organizaciones. Puriq, 4, e196–e196. https://doi.org/10.37073/PURIQ.4.1.196

[18] Tasa-Catanzaro, M. E., Maquera-Quispe, H. G., Rojas-Bujaico, J. F., & Delgado-Rospigliosi, M. G. del C. (2022b). Análisis de información de la gestión de incidentes de seguridad en organizaciones. Puriq, 4, e196–e196. https://doi.org/10.37073/PURIQ.4.1.196

[19] Vivas, G. V., Garcés, F., & Tinoco, W. W. (2017). Seguridades de las Tecnologías de la Información (TI) en el trabajo colaborativo y su aporte a la gobernanza de TI. Revista Científica y Tecnológica UPSE, 4(2), 99–104. https://doi.org/10.26423/RCTU.V4I2.272

[20] Yagual, D. I. Q., Yagual, C. C., & Suárez, I. C. (2022a). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. Revista Científica y Tecnológica UPSE, 9(1), 57–65. https://doi.org/10.26423/RCTU.V9I1.671

[21] Yagual, D. I. Q., Yagual, C. C., & Suárez, I. C. (2022b). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. Revista Científica y Tecnológica UPSE, 9(1), 57–65. https://doi.org/10.26423/RCTU.V9I1.671